FINITE FIELDS AND THEIR APPLICATIONS **3,** 257–274 (1997)
ARTICLE NO. FF970185

On Towers and Composita of Towers of Function Fields over Finite Fields

Arnaldo Garcia

Instituto de Matemática Pura e Aplicada IMPA, Estrada Dona Castorina 110, 22460-320

and

Henning Stichtenoth and Michael Thomas

Mathematik und Informatik, Universität GH Essen, FB 6, D-45117 Essen, Germany
E-mail: stichtenoth@uni-essen.de

Communicated by Michael Tsfasman

Received October 29, 1996

For a tower $F_1 \subseteq F_2 \subseteq \cdots$ of algebraic function fields $F_i/\mathbb{F}_q$, define $\lambda = \lim_{i\to\infty} N(F_i)/g(F_i)$, where $N(F_i)$ is the number of rational places and $g(F_i)$ is the genus of $F_i/\mathbb{F}_q$. The tower is said to be asymptotically good if $\lambda > 0$. We give a very simple explicit example of an asymptotically good tower for all non-prime fields $\mathbb{F}_q$. In this example, all steps F_{i+1}/F_i are tamely ramified Kummer extensions. We then show that any function field $F/\mathbb{F}_q$ having at least one rational place can be embedded into an asymptotically good tower, and we study the behaviour of λ in the compositum of a tower $F_1 \subseteq F_2 \subseteq \cdots$ with an extension E/F_1.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field with q elements. An algebraic function field $F/\mathbb{F}_q$ is an extension of the rational function field $\mathbb{F}_q(x)$ of finite degree $[F:\mathbb{F}_q(x)] < \infty$ such that $\mathbb{F}_q$ is algebraically closed in F. We denote by $N(F)$ the number of rational places (= places of degree one) of $F/\mathbb{F}_q$, and by $g(F)$ the genus of the function field.

A famous theorem of A. Weil asserts that

$$N(F) \leq q + 1 + 2g(F) \cdot \sqrt{q}. \tag{1}$$

1071-5797/97 $25.00

Ihara observed that this bound can be improved considerably if the genus is large with respect to q; see [6, 9, 11]. An "asymptotic" bound was obtained by Drinfeld and Vladut: setting $N_q(g) = \max\{N(F) \mid F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g\}$, and

$$A(q) = \limsup_{g\to\infty} N_q(g)/g,$$

the Drinfeld–Vladut bound states that

$$A(q) \le \sqrt{q} - 1. \tag{2}$$

Note that (1) implies only the much weaker estimate $A(q) \le 2\sqrt{q}$. If q is a square, Ihara [6] and Tsfasman *et al.* [12] proved that in fact

$$A(q) = \sqrt{q} - 1 \qquad (\text{if } q \text{ is a square}). \tag{3}$$

This result has striking applications in coding theory [13]. It was obtained by considering specific sequences of modular curves that have many rational points in comparison to their genus.

If q is not a square, the exact value of $A(q)$ is unknown. Serre [10] showed that

$$A(q) \ge c \cdot \log q > 0 \qquad (\text{for all } q) \tag{4}$$

with some small constant $c > 0$. For some values of q, one has better lower bounds for $A(q)$, see [7, 8, 14, 15]. All these lower bounds were obtained by constructing appropriate infinite classfield towers, resp. modular curves.

A *tower of function fields* over $\mathbb{F}_q$ is a sequence $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ of function fields $F_i/\mathbb{F}_q$ having the following properties:

(i) $F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots$.

(ii) For every $n \ge 1$, the extension F_{n+1}/F_n is separable of degree $[F_{n+1}:F_n] > 1$.

(iii) $g(F_j) > 1$, for some $j \ge 1$.

By the Hurwitz genus formula, (ii) and (iii) imply that $g(F_n) \to \infty$, and it is easily shown that for any tower $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ the sequence $(N(F_n)/g(F_n))_{n\ge1}$ is convergent, cf. [5]. We set

$$\lambda(\mathscr{F}) = \lim_{n\to\infty} N(F_n)/g(F_n). \tag{5}$$

As $0 \le \lambda(\mathscr{F}) \le A(q)$, any tower of function fields over $\mathbb{F}_q$ provides a

lower bound for $A(q)$. We call $\mathcal{F}$ *asymptotically good* (resp. *asymptotically optimal*) if $\lambda(\mathcal{F}) > 0$ (resp. if $\lambda(\mathcal{F}) = A(q)$). Recently, Garcia and Stichtenoth [3, 5] gave explicit constructions of two asymptotically optimal towers $\mathcal{F} = (F_1, F_2, F_3, \ldots)$ over $\mathbb{F}_q$ when $q = l^2$ is a square. In both towers, all extensions F_{n+1}/F_n are wildly ramified Artin–Schreier extensions (i.e., F_{n+1}/F_n is a Galois extension whose Galois group is elementary abelian of exponent $p = \text{char}(\mathbb{F}_q)$, and there are places of F_n which are ramified in F_{n+1}/F_n).

In Section 2, we give very simple constructions of some asymptotically good towers of function fields over $\mathbb{F}_q$ for all $q = p^e$ with $e > 1$ (where p is the characteristic of $\mathbb{F}_q$). In these new towers, the extensions F_{n+1}/F_n are tamely ramified Kummer extensions for all $n \geq 1$. Although simple, two of the towers constructed here are optimal (one for $q = 4$ and the other one for $q = 9$).

Given a tower $\mathcal{F} = (F_1, F_2, F_3, \ldots)$ over $\mathbb{F}_q$ and a finite extension $E \supseteq F_1$, one can consider the compositum tower $\mathcal{E} = (E_1, E_2, E_3, \ldots)$ with $E_i = E \cdot F_i$. In Section 3, we study relations between the corresponding limits $\lambda(\mathcal{F})$ and $\lambda(\mathcal{E})$.

2. TAME TOWERS

Let $\mathbb{P}(F)$ be the set of all places of a function field $F/\mathbb{F}_q$. Given a finite extension E/F and a place $P \in \mathbb{P}(F)$, there are finitely many places $P' \in \mathbb{P}(E)$ lying above P; the ramification index of $P'|P$ is denoted by $e(P'|P)$. The extension E/F is said to be tame if $e(P'|P)$ is relatively prime to the characteristic of $\mathbb{F}_q$, for all places $P \in \mathbb{P}(F)$ and all $P'|P$.

THEOREM 2.1. *Let $\mathcal{F} = (F_1, F_2, F_3, \ldots)$ be a tower of function fields over $\mathbb{F}_q$ satisfying the following conditions:*

(i) *All extensions F_{n+1}/F_n are tame.*

(ii) *The set $S = \{P \in \mathbb{P}(F_1) | P$ is ramified in F_n/F_1 for some $n \geq 2\}$ is finite.*

(iii) *The set $T = \{P \in \mathbb{P}(F_1) | \deg P = 1$, and P splits completely in all extensions $F_n/F_1\}$ is non-empty.*

Then $\mathcal{F}$ is asymptotically good, and one has the estimate

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_1) - 2 + s} > 0,$$

where $t := \#T$ and $s := \sum_{P \in S} \deg P$.

Proof. As F_n/F_1 is tame, the degree of the different of F_n/F_1 is given by

$$\deg \mathrm{Diff}\,(F_n/F_1) = \sum_{P\in S}\sum_{P'|P}(e(P'|P)-1)\cdot \deg P'$$

(here P' runs over all places of F_n lying above P). Since

$$\sum_{P'|P} e(P'|P)\cdot \deg P' = [F_n:F_1]\cdot \deg P,$$

we obtain

$$\deg \mathrm{Diff}\,(F_n/F_1) \le [F_n:F_1]\cdot \sum_{P\in S}\deg P = [F_n:F_1]\cdot s.$$

Now the Hurwitz genus formula implies that

$$2g(F_n) \le [F_n:F_1](2g(F_1)-2+s)+2. \tag{6}$$

On the other hand, we have $N(\mathrm{F}_n) \ge t\cdot[F_n:F_1]$ by condition (iii). Therefore

$$\frac{N(F_n)}{g(F_n)} \ge \frac{2t}{2g(F_1)-2+s+2/[F_n:F_1]}$$

for all $n \ge 2$. This shows that

$$\lambda(\mathscr{F}) = \lim_{n\to\infty}\frac{N(F_n)}{g(F_n)} \ge \frac{2t}{2g(F_1)-2+s}.$$

Observe that inequality (6) implies $2g(F_1)-2+s>0$, since $g(F_n)\to\infty$ for $n\to\infty$. ■

Our next aim is to give some explicit examples of towers that satisfy the hypotheses of Theorem 2.1.

THEOREM 2.2. *Let $m>1$ be an integer with $q\equiv 1 \mod m$, and let $S_0\subseteq \mathbb{F}_q$ be a subset of $\mathbb{F}_q$ with $0\in S_0$. Suppose that $f(t)\in\mathbb{F}_q[t]$ is a polynomial whose leading coefficient is an mth power in $\mathbb{F}_q$ satisfying the conditions* (a), (b), *and* (c) *below:*

(a) $f(t) = t^d\cdot f_1(t)$ *with* $f_1(t)\in\mathbb{F}_q[t]$, $f_1(0)\neq 0$ *and* $\gcd(d,m)=1$.

(b) $\deg f(t) = m$.

(c) *For each* $\alpha \in S_0$, *all roots of the equation* $f(t) = \alpha^m$ *belong to* S_0.

We define function fields $F_n/\mathbb{F}_q$ $(n \geq 1)$ *recursively by* $F_1 := \mathbb{F}_q(x_1)$ *and* $F_{i+1} := F_i(x_{i+1})$ *with*

$$x_{i+1}^m = f(x_i) \qquad (\textit{for } i \geq 1). \tag{7}$$

Then $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ *is a tower of function fields over* $\mathbb{F}_q$ *having the following properties:*

(i) F_{i+1}/F_i *is a tame extension of degree* m, *for every* $i \geq 1$.

(ii) *Let* $P \in \mathbb{P}(F_1)$ *be ramified in* F_n/F_1, *for some* $n \geq 2$. *Then* P *is a zero of* $x_1 - \alpha$ *for some* $\alpha \in S_0$.

(iii) *The pole* P_∞ *of* x_1 *in* F_1 *splits completely in* F_n/F_1, *for every* $n \geq 2$.

(iv) $\lambda(\mathscr{F}) \geq 2/(\#S_0 - 2) > 0$.

Proof. We consider first the extension F_2/F_1, where $F_2 = F_1(x_2)$ and

$$x_2^m = f(x_1) = x_1^d \cdot f_1(x_1). \tag{8}$$

Let $P_1 \in \mathbb{P}(F_1)$ be the zero of x_1 in F_1 and let $P_2 \in \mathbb{P}(F_2)$ be a place lying above P_1. If v_2 denotes the corresponding discrete valuation of F_2, we have from (8):

$$m \cdot v_2(x_2) = d \cdot v_2(x_1) = d \cdot e(P_2|P_1).$$

As gcd $(d, m) = 1$, this implies $[F_2 : F_1] = m = e(P_2|P_1)$ and $v_2(x_2) = d$. We see by induction that $[F_n : F_1] = m^{n-1}$, that P_1 is totally ramified in F_n/F_1 and that $v_n(x_n) = d^{n-1}$ (where v_n is the valuation of F_n corresponding to the unique place $P_n \in \mathbb{P}(F_n)$ lying above P_1). In particular it follows that $\mathbb{F}_q$ is algebraically closed in F_n. Since F_{i+1}/F_i is a cyclic extension of degree m (this follows from Eq. (7) and from $q \equiv 1 \bmod m$), the extension F_{i+1}/F_i is tame.

Next we show by induction that the pole of x_1 splits completely in F_n/F_1. Let $Q \in \mathbb{P}(F_n)$ be a pole of x_1. Then Q is a pole of $x_1, x_2, \ldots, x_n$, by Eq. (7), and

$$x_{n+1}^m = x_n^d \cdot f_1(x_n).$$

Dividing by x_n^m and setting $u := x_{n+1}/x_n$, we obtain

$$u^m = \frac{f_1(x_n)}{x_n^{m-d}} = \beta + z, \tag{9}$$

where β is the leading coefficient of $f(t)$ and the function z has a zero at the place Q. The reduction of Eq. (9) modulo Q gives $u^m \equiv \beta \bmod Q$, and since the equation $t^m = \beta$ has m distinct roots in $\mathbb{F}_q$, the place Q splits completely in F_{n+1}/F_n (we have used Kummer's theorem [11, III.3.7]). As a consequence, we have $N(F_n) \geq m^{n-1}$ and therefore $g(F_n) \to \infty$ for $n \to \infty$.

So far we have proved that $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ is a tower of function fields over $\mathbb{F}_q$ with the properties (i) and (iii) of Theorem 2.2. Now we prove property (ii). Suppose that $P \in \mathbb{P}(F_1)$ is ramified in F_n/F_1. Choose $Q \in \mathbb{P}(F_n)$ with $e(Q|P) > 1$ and let $P_i = Q \cap F_i$ be the restriction of Q to F_i. Since $Q|P$ is ramified, then $P_{i+1}|P_i$ is ramified for some i. From the equation

$$x_{i+1}^m = f(x_i) \tag{10}$$

and from the ramification theory of Kummer extensions [11, III.7.3], it follows that P_{i+1} is a zero of x_{i+1}. Denoting by $z(Q)$ the residue class of an element $z \in F_n$ modulo Q, we obtain from Eq. (10):

$$f(x_i(Q)) = x_{i+1}(Q)^m = 0.$$

Condition (c) of Theorem 2.2 implies that $x_i(Q) \in S_0$. Repeating this argument, we see that $x_{i-1}(Q) \in S_0, \ldots, x_2(Q) \in S_0$, and finally $x_1(Q) \in S_0$. Hence property (ii) is proved.

Now we can apply Theorem 2.1. We set

$$S = \{P \in \mathbb{P}(F_1) | P \text{ is a zero of } x_1 - \alpha \text{ for some } \alpha \in S_0\}$$

and

$$T = \{\text{the pole of } x_1 \text{ in } F_1\}.$$

Theorem 2.1 yields immediately that

$$\lambda(\mathscr{F}) \geq \frac{2}{\#S_0 - 2}. \quad \blacksquare$$

The two subsequent examples were announced (without proof) in [4]. In both examples, the leading coefficient of $f(t)$ is -1, which is an mth power in the corresponding field $\mathbb{F}_q$.

EXAMPLE 2.3. *Let $q = p^e$ with $e > 1$ and $m = (q-1)/(p-1)$. Let $F_n = \mathbb{F}_q(x_1, \ldots, x_n)$ with*

$$x_{i+1}^m + (x_i + 1)^m = 1 \qquad (i = 1, \ldots, n-1).$$

Then $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ is an asymptotically good tower over $\mathbb{F}_q$ with

$$\lambda(\mathscr{F}) \geq \frac{2}{q-2}.$$

Proof. Let $S_0 := \mathbb{F}_q$ and $f(t) := 1 - (t+1)^m$. Conditions (a) and (b) of Theorem 2.2 hold obviously. In order to verify condition (c), let $\alpha \in \mathbb{F}_q$ and take a root γ of the equation $f(t) = \alpha^m$; i.e.,

$$(\gamma + 1)^m = 1 - \alpha^m.$$

If $\alpha^m = 1$ then $\gamma = -1 \in \mathbb{F}_q$. If $\alpha^m \neq 1$ then $1 - \alpha^m \in \mathbb{F}_p \backslash \{0\}$ (observe that $\alpha \mapsto \alpha^m$ is the norm map from $\mathbb{F}_q$ to $\mathbb{F}_p$). Hence

$$(\gamma + 1)^{q-1} = ((\gamma + 1)^m)^{p-1} = (1 - \alpha^m)^{p-1} = 1,$$

and therefore $\gamma + 1 \in \mathbb{F}_q$. Now Theorem 2.2 gives the desired result. ∎

EXAMPLE 2.4. *Let $q = l^2$ be a square and $F_n = \mathbb{F}_q(x_1, \ldots, x_n)$ with*

$$x_{i+1}^{l-1} + (x_i + 1)^{l-1} = 1 \qquad (i = 1, \ldots, n-1).$$

Then $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ is an asymptotically good tower over $\mathbb{F}_q$ with

$$\lambda(\mathscr{F}) \geq \frac{2}{\sqrt{q} - 2}.$$

Proof. Similar to the proof of Example 2.3. Choose $S_0 = \mathbb{F}_l$ and

$$f(t) = 1 - (t+1)^{l-1}. \quad \blacksquare$$

EXAMPLE 2.5. *The extensions F_n/F_1 are not Galois in the two examples above (for $n \geq 3$). We define $\tilde{F}_n$ as the Galois closure of F_n/F_1. The pole of x_1 splits completely in $\tilde{F}_n/F_1$* [11, III.8.4], *hence $\mathbb{F}_q$ is algebraically closed in*

$\tilde{F}_n$. Moreover $\tilde{F}_n/F_1$ is tame, and the only ramified places in $\tilde{F}_n/F_1$ are the places that ramify in F_n/F_1 [11, III.8.4]. *So we can apply Theorem 2.1 and conclude that the tower $\tilde{\mathscr{T}} = (F_1, \tilde{F}_2, \tilde{F}_3, \ldots)$ is asymptotically good over $\mathbb{F}_q$ with*

$$\lambda(\tilde{\mathscr{T}}) \geq \frac{2}{q-2} \qquad \left(\text{resp. } \lambda(\tilde{\mathscr{T}}) \geq \frac{2}{\sqrt{q}-2}\right).$$

Remark 2.6. For $q = 4$, the tower $\mathscr{T}$ of Example 2.3 is asymptotically optimal over $\mathbb{F}_4$, since $\lambda(\mathscr{T}) \geq 2/(q-2) = 1$ and $\lambda(\mathscr{T}) \leq A(4) \leq 1$ (from the Drinfeld–Vladut bound). Elkies [2] observed that in this case ($q = 4$) the tower corresponds in fact to the classical modular curves $X_0(3^n)$, reduced modulo 2.

An analogous remark holds for $q = 9$ in Example 2.4. This tower is asymptotically optimal over $\mathbb{F}_9$ (with $\lambda(\mathscr{T}) = 2$), and it corresponds to the classical modular curves $X_0(2^n)$, reduced modulo 3.

Remark 2.7. Example 2.3 provides a simple and elementary proof that $A(q) > 0$, for all non-prime finite fields. Unfortunately we have not found polynomials $f(t)$ as in Theorem 2.2 over a prime field.

3. COMPOSITA OF TOWERS

We begin with a simple lemma concerning the splitting of places in composita of function fields.

LEMMA 3.1. *Let E/F and F'/F be finite extensions of the function field $F/\mathbb{F}_q$ such that $\mathbb{F}_q$ is algebraically closed in E and in F', and such that F'/F is Galois with $F' \cap E = F$. Suppose that $P \in \mathbb{P}(F)$ is a place of $F/\mathbb{F}_q$ of degree one which splits completely in F'/F, and that $Q \in \mathbb{P}(E)$ is a place of $E/\mathbb{F}_q$ of degree one lying over P. Then the compositum $E' := E \cdot F'$ is Galois over E of degree $[E' : E] = [F' : F]$, the field $\mathbb{F}_q$ is algebraically closed in E', and the place Q splits completely in E'/E.*

Proof. It is well known from Galois theory that E'/E is Galois and that the restriction $\sigma \mapsto \sigma|F'$ yields an isomorphism of the Galois group $\mathrm{Gal}(E'/E)$ onto $\mathrm{Gal}(F'/F)$. We choose a place $Q' \in \mathbb{P}(E')$ which lies over Q, and we set $P' = Q' \cap F'$. Let $\sigma \neq \mathrm{id}$ be a non-trivial automorphism of E'/E. Then

$$\sigma Q' \cap F' = \sigma Q' \cap \sigma F' = \sigma(Q' \cap F') = \sigma P' \neq P',$$

since P splits completely in F'/F. Hence $\sigma Q' \neq Q'$, and Q splits completely in E'/E. It follows in particular that $\deg Q' = 1$ and that $\mathbb{F}_q$ is algebraically closed in E'. ■

Now we consider a tower $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ of function fields over $\mathbb{F}_q$. Let E be a finite separable extension field of F_1. For convenience we assume that $E, F_1, F_2, \ldots$ are all contained in a fixed algebraically closed field Ω. Suppose that $\mathbb{F}_q$ is algebraically closed in the compositum $E_n = E \cdot F_n$, for all $n \geq 1$. Then we obtain another tower $\mathscr{E} = (E_1, E_2, E_3, \ldots)$ over $\mathbb{F}_q$. As $F_n \subseteq E_n$, the tower $\mathscr{F}$ is a subtower of $\mathscr{E}$ and therefore $\lambda(\mathscr{E}) \leq \lambda(\mathscr{F})$; see [5]. Sometimes one can say more about the relation between $\lambda(\mathscr{F})$ and $\lambda(\mathscr{E})$.

THEOREM 3.2. *Let $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ be a tower of function fields over $\mathbb{F}_q$ having the following properties:*

(i) *F_{n+1}/F_n is Galois for every $n \geq 1$.*

(ii) *The set $T = \{P \in \mathbb{P}(F_1) | \deg P = 1$, and P splits completely in all extensions $F_n/F_1\}$ is non-empty.*

(iii) *$\mathscr{F}$ is asymptotically good; i.e., $\lambda(\mathscr{F}) > 0$.*

Let $E \supseteq F_1$ be a finite separable extension such that $\mathbb{F}_q$ is algebraically closed in E and moreover the fields E and F_n are linearly disjoint over F_1 for each $n \geq 1$. Suppose that the set

$$T' = \{Q \in \mathbb{P}(E) | \deg Q = 1 \quad \text{and} \quad Q \cap F_1 \in T\}$$

is non-empty.

Then the tower $\mathscr{E} = (E_1, E_2, E_3, \ldots)$ with $E_n := E \cdot F_n$ is a tower of function fields over $\mathbb{F}_q$ with

$$\lambda(\mathscr{E}) \geq \frac{\#T'}{g(E) - 1 + [E:F] \cdot (1 + N(F_1)/\lambda(\mathscr{F}))}.$$

In particular, the compositum tower $\mathscr{E}$ is asymptotically good.

Proof. Let $a_n = [F_n : F_1]$ and $r = [E:F]$. From Lemma 3.1 it follows that $\mathscr{E} = (E_1, E_2, E_3, \ldots)$ with $E_n = E \cdot F_n$ is a tower of function fields over $\mathbb{F}_q$ and that each place $Q \in T'$ splits completely in all extensions E_n/E_1. Hence

$$N(E_n) \geq a_n \cdot \#T'. \tag{11}$$

Now we have to estimate the genus $g(E_n)$. Let $0 < \varepsilon < \lambda(\mathscr{F})$. Since $N(F_n)/g(F_n) \geq \lambda(\mathscr{F}) - \varepsilon$, for large values of n, we have

$$g(F_n) \leq \frac{N(F_n)}{\lambda(\mathscr{F}) - \varepsilon} \leq a_n \cdot \frac{N(F_1)}{\lambda(\mathscr{F}) - \varepsilon},$$

for sufficiently large n. Now Castelnuovo's inequality [11, III.10.3] yields

$$\begin{aligned} g(E_n) &\leq a_n \cdot g(E_1) + r \cdot g(F_n) + (r-1)(a_n - 1) \\ &\leq a_n \cdot \left(g(E) - 1 + r\left(1 + \frac{N(F_1)}{\lambda(\mathscr{F}) - \varepsilon}\right)\right), \end{aligned} \tag{12}$$

for large n. Dividing the inequalities (11) and (12) and letting $n \to \infty$, we obtain the desired result

$$\lambda(\mathscr{E}) \geq \frac{\#T'}{g(E) - 1 + [E:F](1 + N(F_1)/\lambda(\mathscr{F}))}. \quad \blacksquare$$

For any asymptotically good tower $\mathscr{H} = (H_1, H_2, H_3, \ldots)$ holds trivially that H_1 has at least one rational place. Now we can show:

THEOREM 3.3. *Suppose that $H/\mathbb{F}_q$ is a function field having at least one rational place. Then there exists an asymptotically good tower $\mathscr{H} = (H_0, H_1, H_2, \ldots)$ of function fields over $\mathbb{F}_q$ with $H_0 = H$.*

Proof. Our starting point is an arbitrary asymptotically good tower $\mathscr{F} = (F_1, F_2, \ldots)$ over $\mathbb{F}_q$ such that all extensions F_{n+1}/F_n are Galois and such that the set

$$T = \{P \in \mathbb{P}(F_1) | \deg P = 1, \quad \text{and} \quad P \text{ splits completely in all } F_n/F_1\}$$

is non-empty. If q is not a prime number, the existence of such a tower follows from Section 2. In the general case, Serre [10] proved that certain classfield towers have these properties (see also [8, 14]). We fix a place $P \in T$, choose an element $x \in F_1$ having P as a simple zero, and set $F_0 := \mathbb{F}_q(x)$. Let Ω be an algebraically closed field containing all fields F_n.

Let $Q_0 \in \mathbb{P}(H)$ be a rational place of $H/\mathbb{F}_q$, and let $z \in H$ be a function having Q_0 as its unique zero. Then the place Q_0 is totally ramified in the extension $H/\mathbb{F}_q(z)$. We embed H into Ω by mapping z to x, and we will identify H with its image under this embedding.

We set $H_n := H \cdot F_n$ for each $n \geq 0$. The place P is unramified in F_1/F_0 (since it is a simple zero of x) and also unramified in all extensions F_n/F_1

(as $P \in T$); it is totally ramified in H_1/F_1 (since x has a unique zero in H), and in particular the unique place of H_1 above P is rational. So the fields H_1 and F_n are linearly disjoint over F_1. By Theorem 3.2 the tower $(H_1, H_2, H_3, \ldots)$ is asymptotically good. ■

From Theorem 3.2 we have a lower bound for $\lambda(\mathscr{E})$ when $\mathscr{E}$ is the compositum of a tower $\mathscr{F}$ with an extension E/F_1. In many cases we can determine precisely the limit $\lambda(\mathscr{E})$.

First we introduce some notation. Given a tower of function fields $\mathscr{F} = (F_1, F_2, F_3, \ldots)$, a place $P \in \mathbb{P}(F_1)$ is said to be ramified in $\mathscr{F}$ if P is ramified in an extension F_n/F_1, for some $n \geq 2$. We set

$$S(\mathscr{F}) := \{P \in \mathbb{P}(F_1) \mid P \text{ is ramified in } \mathscr{F}\}. \tag{13}$$

If $S(\mathscr{F})$ is finite we can define the divisors

$$A_n := \sum_{\substack{P \in \mathbb{P}(F_n) \\ P \cap F_1 \in S(\mathscr{F})}} P. \tag{14}$$

LEMMA 3.4. *For any tower $\mathscr{F}$ of function fields, the sequence*

$$\left(\frac{N(F_n)}{[F_n : F_1]}\right)_{n \geq 1}$$

is monotonously decreasing, and the sequence

$$\left(\frac{g(F_n) - 1}{[F_n : F_1]}\right)_{n \geq 1}$$

is monotonously increasing. If moreover $S(\mathscr{F})$ is finite, the sequence

$$\left(\frac{\deg A_n}{[F_n : F_1]}\right)_{n \geq 1}$$

is also monotonously decreasing.

Proof. (i) We have the trivial inequality $N(F_{n+1}) \leq [F_{n+1} : F_n] \cdot N(F_n)$ and therefore

$$\frac{N(F_{n+1})}{[F_{n+1} : F_1]} \leq \frac{[F_{n+1} : F_n] \cdot N(F_n)}{[F_{n+1} : F_1]} = \frac{N(F_n)}{[F_n : F_1]}.$$

(ii) The Hurwitz genus formula implies that

$$g(F_{n+1}) - 1 \geq [F_{n+1}:F_n](g(F_n) - 1).$$

The monotony of the sequence $((g(F_n) - 1)/[F_n:F_1])_{n\geq 1}$ follows immediately.

(iii) Finally we assume that $S(\mathscr{F})$ is finite, and we consider the sequence $(\deg A_n/[F_n:F_1])_{n\geq 1}$. One has

$$\begin{aligned}\deg A_{n+1} &= \sum_{\substack{P'\in\mathbb{P}(F_{n+1})\\ P'\cap F_1\in S(\mathscr{F})}} \deg P' = \sum_{\substack{P\in\mathbb{P}(F_n)\\ P\cap F_1\in S(\mathscr{F})}} \sum_{P'|P} f(P'|P)\cdot \deg P \\ &\leq \sum_{\substack{P\in\mathbb{P}(F_n)\\ P\cap F_1\in S(\mathscr{F})}} \deg P\cdot [F_{n+1}:F_n] = [F_{n+1}:F_n]\cdot \deg A_n.\end{aligned}$$

Hence the sequence $(\deg A_n/[F_n:F_1])_{n\geq 1}$ is also monotonously decreasing. ■

By Lemma 3.4, we can define:

DEFINITION 3.5. For a tower $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ of function fields over $\mathbb{F}_q$, let

$$\nu(\mathscr{F}) := \lim_{n\to\infty} \frac{N(F_n)}{[F_n:F_1]} \qquad \text{and} \qquad \gamma(\mathscr{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n:F_1]}.$$

If $S(\mathscr{F})$ is finite, let

$$\alpha(\mathscr{F}) := \lim_{n\to\infty} \frac{\deg A_n}{[F_n:F_1]},$$

where A_n is defined by (14).

We have the obvious inequalities

$$\begin{aligned}&0 \leq \nu(\mathscr{F}) \leq N(F_1) < \infty,\\ &0 \leq \alpha(\mathscr{F}) < \infty,\\ &0 < \gamma(\mathscr{F}) \leq \infty.\end{aligned}$$

Note that the tower is asymptotically good (i.e., $\lambda(\mathscr{F}) > 0$) if and only if $\gamma(\mathscr{F}) < \infty$ and $\nu(\mathscr{F}) > 0$, and in this case one has

$$\lambda(\mathscr{F}) = \nu(\mathscr{F})/\gamma(\mathscr{F}).$$

Let H/F be a finite separable extension of function fields over $\mathbb{F}_q$, and let $Q \in \mathbb{P}(H)$ be a place of H. Then $d(Q|Q \cap F)$ denotes the different exponent of Q with respect to the extension H/F; hence the different of H/F is given by

$$\operatorname{Diff}(H/F) = \sum_{Q \in \mathbb{P}(H)} d(Q|Q \cap F) \cdot Q.$$

Now we prove an analogue of the Hurwitz genus formula for composita of towers.

THEOREM 3.6. *Suppose that $\mathscr{T} = (F_1, F_2, F_3, \ldots)$ is a tower of function fields over $\mathbb{F}_q$. Let E/F_1 be a finite separable extension such that E and F_n are linearly disjoint over F_1, and such that $\mathbb{F}_q$ is algebraically closed in $E_n = E \cdot F_n$, for all $n \geq 1$. Denote by $\mathscr{E} = (E_1, E_2, E_3, \ldots)$ the compositum tower of $\mathscr{T}$ and E. Assume that the following conditions hold:*

(i) *$S(\mathscr{T})$ is finite, and $\alpha(\mathscr{T}) = 0$.*

(ii) *All $P \in S(\mathscr{T})$ are tame in E/F_1.*

Then $S(\mathscr{E})$ is finite, and we have

$$2g(E) - 2\gamma(\mathscr{E}) - 2 = [E:F_1](2g(F_1) - 2\gamma(\mathscr{T}) - 2) + \delta,$$

with

$$\delta := \sum_{\substack{Q \in \mathbb{P}(E) \\ Q \cap F_1 \in S(\mathscr{T})}} d(Q|Q \cap F_1) \cdot \deg Q.$$

Proof. $S(\mathscr{E})$ is finite because all places $Q \in \mathbb{P}(E)$ with $Q \cap F_1 \notin S(\mathscr{T})$ are unramified in the tower $\mathscr{E}$. To simplify notation we denote by P (resp. Q, P', Q') the places of F_1 (resp. E, F_n, E_n), and we set $S := S(\mathscr{T})$. The Hurwitz genus formula for the extension E_n/F_1 gives

$$2g(E_n) - 2 = [E_n:F_1](2g(F_1) - 2) + \delta_1 + \delta_2, \tag{15}$$

where

$$\delta_1 := \sum_{P \notin S} \sum_{Q'|P} d(Q'|P) \cdot \deg Q'$$

and

$$\delta_2 := \sum_{P \in S} \sum_{Q'|P} d(Q'|P) \cdot \deg Q'.$$

Using the transitivity of the different in $F_1 \subseteq E \subseteq E_n$ we obtain

$$\begin{aligned}
\delta_1 &= \sum_{P \notin S} \sum_{Q|P} \sum_{Q'|Q} (e(Q'|Q) \cdot d(Q|P) + d(Q'|Q)) \cdot \deg Q' \\
&= \sum_{P \notin S} \sum_{Q|P} \sum_{Q'|Q} d(Q|P) \cdot \deg Q' \\
&= \sum_{P \notin S} \sum_{Q|P} d(Q|P) \cdot \sum_{Q'|Q} f(Q'|Q) \cdot \deg Q \qquad (16) \\
&= [E_n : E] \cdot \sum_{P \notin S} \sum_{Q|P} d(Q|P) \cdot \deg Q \\
&= [E_n : E] \cdot (2g(E) - 2 - [E : F_1](2g(F_1) - 2) - \delta).
\end{aligned}$$

The transitivity of the different in $F_1 \subseteq F_n \subseteq E_n$ yields

$$\begin{aligned}
\delta_2 &= \sum_{P \in S} \sum_{P'|P} \sum_{Q'|P'} (e(Q'|P') \cdot d(P'|P) + d(Q'|P')) \cdot \deg Q' \\
&= \sum_{P \in S} \sum_{P'|P} d(P'|P) \cdot \deg P' \cdot \sum_{Q'|P'} e(Q'|P') \cdot f(Q'|P') \\
&\quad + \sum_{P \in S} \sum_{P'|P} \sum_{Q'|P'} d(Q'|P') \cdot \deg Q' \\
&= [E_n : F_n] \cdot \deg \operatorname{Diff}(F_n/F_1) + \sum_{P \in S} \sum_{P'|P} \deg P' \qquad (17) \\
&\quad \cdot \sum_{Q'|P'} (e(Q'|P') - 1) \cdot f(Q'|P') \\
&= [E : F_1] \cdot (2g(F_n) - 2 - [F_n : F_1](2g(F_1) - 2)) + h(n)
\end{aligned}$$

with

$$h(n) = \sum_{P \in S} \sum_{P'|P} \deg P' \cdot \sum_{Q'|P'} (e(Q'|P') - 1) \cdot f(Q'|P').$$

Note that

$$\frac{h(n)}{[F_n : F_1]} \leq [E_n : F_n] \cdot \frac{1}{[F_n : F_1]} \cdot \deg \left(\sum_{P \in S} \sum_{P'|P} P' \right) = [E : F_1] \cdot \frac{\deg A_n}{[F_n : F_1]},$$

and therefore the assumption $\alpha(\mathscr{F}) = 0$ implies that

$$\lim_{n\to\infty} \frac{h(n)}{[F_n : F_1]} = 0. \tag{18}$$

Now we obtain from (15), (16), and (17) that

$$\begin{aligned}\frac{2g(E_n) - 2}{[E_n : E]} &= [E : F_1](2g(F_1) - 2) \\ &\quad + 2g(E) - 2 - [E : F_1](2g(F_1) - 2) - \delta \\ &\quad + [E : F_1]\left(\frac{2g(F_n) - 2}{[F_n : F_1]} - (2g(F_1) - 2)\right) + \frac{h(n)}{[F_n : F_1]} \qquad (19) \\ &= 2g(E) - 2 - \delta + [E : F_1]\left(\frac{2g(F_n) - 2}{[F_n : F_1]} - (2g(F_1) - 2)\right) \\ &\quad + \frac{h(n)}{[F_n : F_1]}.\end{aligned}$$

For $n \to \infty$ we get from (19), (18), and Definition 3.5 that

$$2\gamma(\mathscr{E}) = 2g(E) - 2 - \delta + [E : F_1](2\gamma(\mathscr{F}) - (2g(F_1) - 2)). \quad \blacksquare$$

COROLLARY 3.7. *Notations and assumptions as in Theorem* 3.6. *Assume moreover that the tower $\mathscr{F}$ is asymptotically good. Then*

$$\lambda(\mathscr{E}) = \frac{\nu(\mathscr{E})}{g(E) - 1 - \delta/2 + [E : F_1](\gamma(\mathscr{F}) - g(F_1) + 1)}.$$

Proof. Since $\mathscr{F}$ is asymptotically good, $\gamma(\mathscr{F}) < \infty$ and, *a fortiori,* $\gamma(\mathscr{E}) < \infty$ by Theorem 3.6. Therefore $\lambda(\mathscr{E}) = \nu(\mathscr{E})/\gamma(\mathscr{E})$. Substituting the formula for $\gamma(\mathscr{E})$ given in Theorem 3.6, we obtain the desired result. $\blacksquare$

The assumptions of Theorem 3.6 hold trivially when the tower $\mathscr{F}$ is unramified (i.e., $S(\mathscr{F}) = \varnothing$). Now we give a more interesting (and less trivial) application of Theorem 3.6 and Corollary 3.7.

EXAMPLE 3.8. *Let $q = l^2$ be a square. Consider the tower $\mathscr{F} = (F_1, F_2, F_3, \ldots)$ over $\mathbb{F}_q$ which is defined by $F_1 = \mathbb{F}_q(x_1)$ and $F_{n+1} = F_n(z_{n+1})$, where z_{n+1} satisfies the equation*

$$z_{n+1}^l + z_{n+1} = x_n^{l+1}, \qquad \text{with } x_n = \frac{z_n}{x_{n-1}} \text{ (for } n \geq 2).$$

This tower was studied in [3]. It has the following properties:

(i) $[F_n : F_1] = l^{n-1}$, see [3, Lemma 2.2].

(ii) For $q \equiv 1 \bmod 2$ and $n \geq 3$, one has

$$N(F_n) = (l^2 - 1) \cdot l^{n-1} + 2l,$$

and for $q \equiv 0 \bmod 2$ and $n \geq 5$, one has

$$N(F_n) = (l^2 - 1) \cdot l^{n-1} + 2l^2,$$

see [3, Remark 3.4].

(iii) The genus of F_n is given by

$$g(F_n) = \begin{cases} l^n + l^{n-1} - l^{(n+1)/2} - 2l^{(n-1)/2} + 1, & \text{if } n \equiv 1 \bmod 2, \\ l^n + l^{n-1} - \frac{1}{2}l^{n/2+1} - \frac{3}{2}l^{n/2} - l^{n/2-1} + 1, & \text{if } n \equiv 0 \bmod 2; \end{cases}$$

see [3, Theorem 2.10].

(iv) $S(\mathscr{F}) = \{P_0, P_\infty\}$ where P_0 (resp. P_∞) is the zero (resp. the pole) of x_1 in the rational function field $F_1 = \mathbb{F}_q(x_1)$. The place P_∞ is totally ramified in all extensions F_n/F_1. See [3, Lemma 2.9, Prop. 1.1 and Lemma 2.1].

(v) The divisor A_n as defined by Eq. (14) has degree

$$\deg A_n = \begin{cases} 2l^{(n-1)/2}, & \text{if } n \equiv 1 \bmod 2, \\ l^{n/2} + l^{n/2-1}, & \text{if } n \equiv 0 \bmod 2. \end{cases}$$

See [3, Lemma 2.9].

(vi) Let $P \in \mathbb{P}(F_1)$ be the zero of $x_1 - \beta$, with $0 \neq \beta \in \mathbb{F}_q$. Then P splits completely in all extensions F_n/F_1, see [3, Sec. 3].

From these facts we obtain immediately that

$$\alpha(\mathscr{F}) = 0,\ \nu(\mathscr{F}) = l^2 - 1,\ \gamma(\mathscr{F}) = l + 1, \text{ and } \lambda(\mathscr{F}) = l - 1.$$

We consider now a finite separable extension E/F_1, where $\mathbb{F}_q$ is algebraically closed in E_1 and the places P_0 and P_∞ are tame in E/F_1. As P_∞ is totally ramified in the extension F_n/F_1, the fields E and F_n are linearly disjoint over F_1, and $\mathbb{F}_q$ is algebraically closed in $E_n = E \cdot F_n$ for all $n \geq 1$. Let $\mathscr{E} = (E_1, E_2, E_3, \ldots)$ denote the compositum tower. We set

$$Z := \{Q \in \mathbb{P}(E) | Q \text{ is a zero or a pole of } x_1\}$$

and

$$N_0(E) := \#\{Q \in \mathbb{P}(E) | \deg Q = 1 \text{ and } Q \notin Z\}.$$

Since P_0 and P_∞ are tame in E/F_1, the different exponent of a place $Q \in Z$ with respect to the extensions E/F_1 is given by

$$d(Q|Q \cap F_1) = |v_Q(x_1)| - 1.$$

We have

$$\nu(\mathscr{E}) = N_0(E),$$

as follows easily from (v), (vi), and Lemma 3.1. Corollary 3.7 yields in this situation the formula

$$\lambda(\mathscr{E}) = \frac{N_0(E)}{g(E) - 1 + [E:F_1](l+2) - \frac{1}{2}\sum_{Q \in Z} |v_Q(x_1) - 1| \cdot \deg Q}. \quad (20)$$

Remark 3.9. Consider the set

$$\Lambda(q) = \{\lambda \in \mathbb{R} | \text{ there is a sequence of function fields } F_n/\mathbb{F}_q \text{ with } \lim_{n\to\infty} N(F_n)/g(F_n) = \lambda\}.$$

For $q = l^2$ a square number, $\Lambda(q)$ is a subset of the interval $[0, l-1] \subseteq \mathbb{R}$ with $0 \in \Lambda(q)$ and $l - 1 \in \Lambda(q)$. Using formula (20) one can construct many real numbers $\lambda \in \Lambda(q)$, by an appropriate choice of the extension E/F_1.

REFERENCES

1. V. G. Drinfeld and S. G. Vladut, Number of points of an algebraic curve, *Funct. Anal.* **17** (1983), 53–54.
2. N. Elkies, Beyond Goppa codes, preprint, 1996.
3. A. Garcia and H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, *Invent. Math.* **121** (1995), 211–222.
4. A. Garcia and H. Stichtenoth, Asymptotically good towers of function fields over finite fields, *C.R. Acad. Sci. Paris Ser. I Math.* **322** (1996), 1067–1070.
5. A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61,** (1996), 248–273.
6. Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), 721–724.

7. M. Perret, Tours ramifiées infinies de corps de classes, *J. Number Theory* **38** (1991), 300–322.
8. R. Schoof, Algebraic curves over $\mathbb{F}_2$ with many rational points, *J. Number Theory* **41** (1992), 6–14.
9. J.-P. Serre, Sur le nombre des points d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris Ser. I Math.* **269** (1983), 397–402.
10. J.-P. Serre, Rational points on curves over finite fields, Lecture Notes, Harvard University, 1985.
11. H. Stichtenoth, "Algebraic Function Fields and Codes," Springer Universitext, Berlin/Heidelberg/New York, Springer, 1993.
12. M. A. Tsfasman, S. G. Vladut, and T. Zink, Modular curves, Shimura curves and Goppa codes, better than the Varshamov–Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.
13. M. A. Tsfasman and S. Vladut, "Algebraic–Geometric Codes," Kluwer, Dordrecht, 1991.
14. C. P. Xing, Multiple Kummer extensions and the number of prime divisors of degree one in function fields, *J. Pure Appl. Algebra* **84** (1993), 85–93.
15. T. Zink, Degeneration of Shimura surfaces and a problem in coding theory, *in* "Fundamentals of Computation Theory" (L. Budach, Ed.), pp. 503–511, Springer Lecture Notes in Computer Science, Vol. 199, Springer, New York, 1985.